


CONFIDENTIALITY AND
SECURITY POLICIES AND
PROCEDURES
FOR
PEMS CLIENT-LEVEL DATA
[AN OVERVIEW FOR **PEMS** USERS]

HOW TO NAVIGATE THIS PRESENTATION

- To move from slide to slide, either click the left button of your mouse or use the scroll on your mouse
- Throughout this presentation, you will see places that say “click here” in order to see more information on the topic.
- When you come to one of these places, click on the word “here” with your mouse and that will bring you to another slide
- Move the mouse over the word “back” until the mouse arrow becomes a hand, and then click the left mouse button on “back.” BE SURE only to click with the hand, otherwise you will be directed to the wrong slide.

WHAT IS  PEMS ?

WHAT IS PEMS?

1. PEMS stands for the Program Evaluation and Monitoring System
2. PEMS is an internet browser-based software for data entry and reporting
3. If an agency receives funding from the Centers for Disease Control (CDC) for HIV prevention programs, that agency must collect data for PEMS
4. There are two types of data to be collected:
 - Data that describes a program being funded
 - Data that describes the clients being served

BECOMING A PEMS USER

BECOMING A PEMS USER

1. A PEMS user is a staff member who will have access to PEMS client-level data for the purposes of collecting, processing or analyzing that data
2. In order to be authorized to be a PEMS user, you must do the following:
 - Sign a confidentiality statement. Click [here](#).
 - Sign a statement of acknowledgement and agreement of the PEMS confidentiality and security policy. Click [here](#).
 - Take the PEMS Confidentiality and Security Quiz, and review the correct answers to assure you understand any errors
(you must give all three of these documents to your supervisor)

PEMS CLIENT-LEVEL DATA

PEMS CLIENT-LEVEL DATA IS:

1. Information that is collected about a particular client while the client is enrolled in your program
2. For the purposes of PEMS, this data could be:
 - Client demographics – such as the race, ethnicity, gender or year of birth of the client
 - Client risk-behaviors – such as whether the client has had sex or used injection drugs during a certain period of time
3. The official definition of PEMS Client-Level Data for the purposes of this policy can be viewed by clicking [here](#)

PEMS CLIENT-LEVEL DATA IS:

4. PEMS client-level data records can consist of either:
 - o Paper Records – client-level data that is on a data collection form for example
 - o Electronic Records – client-level data that is stored electronically (on a computer most likely).
 - o Portable Electronic Records – client-level data that is stored on portable electronic devices such as a laptop, blackberry etc., or on removable storage media such as a diskette or CD etc.

PEMS AND CONFIDENTIALITY

PEMS AND CONFIDENTIALITY

1. After learning what PEMS Client-Level Data is, you can see how it could be possible to use this data to identify a particular client.
2. For this reason, it is very important that this data be kept confidential in order to protect client privacy. Click [here](#) to see the definition of confidentiality.
3. The document which these slides summarizes contains policies to assure that we are all protecting the Client-Level data that is collected for PEMS.

SECURING PEMS CLIENT-LEVEL DATA

SECURING PEMS CLIENT-LEVEL DATA

1. When client-level data is not being used, it must be stored in a secured area. A secured area is a locked file cabinet or other locked receptacle within a room that has floor-to-ceiling walls and a door with a lock.
 - o For the purpose of talking about client-level data, a secured area would just be a room with floor-to-ceiling walls and a door with a lock
2. Secured Areas must be locked when the PEMS user is not present.

PEMS

CLIENT-LEVEL DATA IN A SECURE AREA

PEMS CLIENT-LEVEL DATA IN A SECURE AREA: **PASSWORDS, KEYS, ETC...**

1. As a PEMS user, you are responsible for protecting any keys, passwords/codes or electronic devices that would give a person access to PEMS client-level data. All of these must be kept in a locked location.
2. If you discover that a password has been stolen or become known to another person, notify your supervisor immediately. This would be a security breach.

PEMS CLIENT-LEVEL DATA IN SECURED AREA: **COMPUTERS**

1. If client-level data is stored on a computer, the computer must:
 - o Have an automatic screen saver lock with a 15 minute or less activation time
 - o Be password protected (you need a username and password to unlock the screensaver)
 - o Be locked at all times when not in use
 - o Be located in a secured area
 - o Be protected by surge suppressors and emergency battery power to prevent data loss in case of power fluctuations

PEMS CLIENT-LEVEL DATA IN A SECURED AREA: VISITORS

1. If a person who is not a PEMS user is in a secured area, they must be accompanied at all times, and client-level data must be removed from view
2. Regular maintenance personnel must sign a confidentiality statement before being admitted to a secured area

PEMS CLIENT-LEVEL DATA: LEAVING

1. If you are leaving a secured area for a brief time (less than 30 minutes)
 - o Client-level data records must be turned face-down on office surfaces
 - o Computers storing client-level data records must be locked
2. If you are leaving a secured area for a long time (more than 30 minutes)
 - o Client-level data records must be returned to their locked file cabinet or receptacle
 - o Computers storing client-level data records must be locked

PEMS CLIENT-LEVEL DATA IN THE FIELD

PEMS CLIENT-LEVEL DATA IN THE FIELD:

COLLECTING DATA

1. If you are in the field and need to collect client-data from a client verbally you must:
 - o Make sure a door can be closed
 - o Make sure you are alone in the room with the client or that only PEMS users are present
2. If you are in the field and a client will be completing a client-level data form individually you must:
 - o Assure that you are in a room with a door
 - o Do your best to honor client requests to complete a form in a more private location

PEMS CLIENT-LEVEL DATA IN THE FIELD: HANDLING DATA

1. When you have client-level data records in the field:
 - o Keep records in a manila envelope that is sealed and marked 'confidential' or in a locked briefcase
 - o Do not leave records unattended
 - o Do not keep records overnight (except with prior approval from the PEMS System Administrator – click [here](#).)
 - o Encrypt portable electronic records. Click [here](#) for a definition of encryption.

PEMS CLIENT-LEVEL DATA: RETENTION AND DISPOSAL

CLIENT-LEVEL DATA:

RETENTION AND DISPOSAL

1. Paper client-level data records:
 - o You must keep these records for 6 years from the date that they were created
 - o After that point, they must be machine shredded
2. Portable electronic records:
 - o You should only keep these records for as long as it takes to complete the task that they were created for
 - o After that point, disks and other storage media must be sanitized
3. Electronic records:
 - o Electronic records stored on a computer hard-drive can be kept indefinitely
 - o Before you get rid of a computer that has client-level data stored on it, or give to someone who is not a PEMS user, the hard drive must be sanitized

TRANSMITTING CLIENT-LEVEL DATA

TRANSMITTING CLIENT LEVEL DATA: MAIL, EMAIL

1. When transmitting client-level data using the U.S. Mail you must:
 - o Place data in an envelope stamped 'confidential'
 - o Address the envelope to the PEMS System Administrator (see pg.10 of the policy for the address).
2. Email
 - o You must NOT send client-level data through email
 - o The exception to this is the random referral code – in this case you must use the confidentiality notice on pg.10 of the policy

TRANSMITTING CLIENT LEVEL DATA: FAX

1. You must not fax client-level data unless you have prior authorization from the PEMS System Administrator
2. Fax machines being used must be located in secured areas
3. After assuring these two things, you must do the following when faxing:
 - o Use a coversheet with the confidentiality notice on pg.10 of the policy
 - o Call the person the fax is going to before you send it in order to tell them
 - o Confirm and re-check the fax number on the view screen
 - o Call the person you sent the fax to in order to verify that they got it
 - o If data was not received attempt to retrieve it

PRINTING AND PHOTOCOPING CLIENT-LEVEL DATA

PRINTING **AND** PHOTOCOPING CLIENT-LEVEL **DATA**

1. Both printers and photocopiers must be located in secured areas
2. To print or photocopy:
 - o Wait by the machine until the job is completed
 - o Do not print or photocopy if there are people in the area who are not PEMS users

VERBAL DISCUSSION ABOUT CLIENT-LEVEL DATA

VERBAL DISCUSSION ABOUT CLIENT-LEVEL DATA

1. Do not discuss client-level data with anyone who is not a PEMS user
2. Do not discuss client-level data when non-PEMS users may be able to overhear
3. When discussing client-level data on the telephone:
 - o Only do so with familiar PEMS users or a referral agency
 - o Only do so within a secured area
 - o Attempt to prevent non-PEMS users from overhearing

PEMS USER RESPONSIBILITIES

PEMS USER RESPONSIBILITIES

1. As a PEMS user, you have the following responsibilities to avoid a breach of confidentiality: (Click [here](#) to see the definition of a breach)
 - o Adhere to policies in this document to ensure confidentiality of client-level data that you work with
 - o Do not access client-level data that is not necessary to do your job
 - o Do not disclose any client-level data to non-PEMS users
 - o Challenge unauthorized users of data
 - o Report suspected security and confidentiality breaches to your supervisor

PEMS USER RESPONSIBILITIES

Not adhering to these responsibilities could result in the following penalties:

- o Reprimands
- o Suspension of system and data privileges
- o Suspension from duty
- o Civil penalties
- o Criminal prosecution

RELEASE OF CLIENT-LEVEL DATA

RELEASE OF CLIENT DATA

1. Releasing client-level data means giving that data to an individual or organization other than the Vermont Department of Health or the CDC
2. Any request that you get for client-level data from an individual or agency outside of your own must be forwarded to the PEMS System Administrator
3. However, you are allowed to release referral codes to other agencies that get money from the Vermont Department of health in order to track referrals

END.

THANK YOU!

*please complete the **PEMS** confidentiality and security quiz now.

PEMS User Confidentiality Statement

As a person who will have access to PEMS client-level data in order to fulfill my responsibilities, I hereby acknowledge that my access to this data shall be restricted as follows:

1. I understand that all information as to personal facts and circumstances obtained in connection with the PEMS client-level data must be held confidential and be considered privileged communications
2. I shall hold in confidence any information about persons which comes to my attention through my access to PEMS client-level data
3. I shall not divulge or disclose this information in any manner whatsoever to an unauthorized person without the written permission of the PEMS System Administrator.
4. I shall access only those PEMS client-level data records that I must collect, process or analyze in fulfillment of my responsibilities
5. I shall challenge any unauthorized users of the data and report suspected security and confidentiality breaches to my direct supervisor or the PEMS System Administrator

Additionally, I understand that I may be subject to reprimands, suspension of system privileges/data access privileges, suspension from duty, civil penalties or criminal prosecution for any of the following acts:

1. Failure to ensure the confidentiality of the PEMS client-level data records to which I have access by:
 - a. Failing to adhere to the policies and procedures in the document entitled "Confidentiality and Security Policies and Procedures for PEMS Client Level Data"
 - b. Otherwise causing the disclosure of any PEMS client-level data to an unauthorized person
2. Accessing records that are not necessary for fulfillment of my responsibilities as a PEMS user
3. Failing to challenge unauthorized use of PEMS client-level data
4. Failing to report a suspected breach of security or confidentiality to a supervisor or the System Administrator.

Upon concluding my work as a PEMS user at {insert agency name}, I hereby agree to return to {insert agency name} all records and copies thereof that I obtained in connection with my work as a PEMS user. Furthermore, I agree to keep confidential all information contained in the records to which I had access during my work as a PEMS user at {insert agency name}.

(PRINT) Last Name

First

MI

Signature

Date _____

Witness Signature

Date _____

back

Acknowledgement and Agreement of Confidentiality and Security Policies and Procedures for PEMS Client-Level Data

I have reviewed the Power Point slide presentation entitled “Confidentiality and Security Policies and Procedures for PEMS Client-Level Data – An Overview for PEMS Users” and completed the related quiz and I agree to comply with the terms and conditions governing the appropriate and allowed use of PEMS client-level data as defined by the Confidentiality and Security Policies and Procedures for PEMS Client-Level Data.

I agree to abide by the procedures stated in this document.

(Signature)

(Printed Name)

[back](#)

PEMS CLIENT-LEVEL DATA

Any record containing PEMS constructive identifying information

PEMS CONSTRUCTIVE IDENTIFYING INFORMATION

Any single piece of information or combination of several pieces of information from PEMS that could be used to deduce the identity of an individual (e.g, names or pieces of names, addresses, ZIP codes, telephone numbers, ethnicity, gender)

[back](#)

CONFIDENTIALITY:

Disclosure of personal information in a relationship of trust and with the expectation that it will not be divulged to others in ways that are inconsistent with the original disclosure

[back](#)

ENCRYPTION:

The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to *decrypt* it.

[back](#)

THE **SYSTEM** ADMINISTRATOR

Who is the System Administrator?

- o Ashley Dutro at the Vermont Department of Health

What are the roles of the System Administrator?

- o Responsible for security of the PEMS data and database
- o Ensuring staff training
- o Reviewing and updating this policy
- o Receiving complaints about this policy

[back](#)

BREACH

Infraction or violation of a standard, obligation or law. A breach in data security would include any unauthorized use of data, even data without names. A breach, in its broadest sense, may be caused by an act of God, a person, or an application/system and may be malicious in nature or purely unintended.

A breach does not necessarily mean that sensitive information was released to the public or that any one person was harmed. A minor infraction, like forgetting to lock a file drawer containing sensitive information – even if inside the secured area – constitutes a breach of security protocol as compared to a breach of confidentiality.

BREACH OF CONFIDENTIALITY

A security infraction that results in the release of private information with or without harm to one or more individuals.

[back](#)